Mutual Networked Device Authentication Based Upon Unique Gravitational Conditions at Location of Fixed-Position Secure Systems via Precision Miniaturized Timekeeping

25 September 2023

Simon Edwards
Research Acceleration Initiative

Introduction

Next Generation (H6) atomic timekeeping, given its compact size and non-reliance upon decay events for timekeeping at levels of precision well-beyond the capabilities of current-generation atomic clocks, has many unexplored applications not previously considered given the onerous size and power consumption of previous systems.

Simplistic yet secure methods are required for mutual authentication of nodes, particularly those unlikely to be anticipated by adversaries. Miniaturized precision timekeeping has unexplored application in the area of networked device authentication, particularly in the case of systems the geospatial position of which are fixed.

Abstract

By integrating an H6 clock into all possible secure terminals and mainframes and creating a baseline for drift in the measured time as tracked by each of these clocks relative to both Naval Observatory time and to one another, it is possible for computers on secure networks to identify when an unauthorized user is masquerading as a legitimate node. Legitimate nodes should have timecode that deviates from Naval Observatory time to an extent (relative to the length of time the clock has been running) that is determined by the unique gravitational conditions at the site of the computer or mainframe.

As these precise gravitational conditions would be impossible for an adversary to reproduce and as these timecodes consist of numbers that are hundreds of digits long, an unauthorized user would not be able to make heads or tails of the hyper-precise timecode or make use of snapshots of this timecode in order to impersonate authentic users. This type of security system is highly useful given its simplicity and its ability to enable any and all nodes on a secure network to know immediately if any communication is inauthentic.

Measurements of connection latency (ping) are rough estimates and are rarely accurate to even the millisecond, although they are frequently measured in milliseconds. Without the ability to accurately assess latency, an adversary operating half a world away would have a very difficult time, indeed, trying to determine a 100-digit system timecode's relative position to variable network latency.

Only a local system pre-programmed with authentic systems' temporal drift profiles would be able to determine if traffic were authentic.

As these nodes would have the same latency-estimation issues that an outsider might, it is necessary for the timecodes of each system in communication with one another to simultaneously transmit their codes to one another without waiting for delivery confirmation or handshakes and for the length of time it takes for a signal to travel in either direction to be symmetrical. As these times are, under controlled network conditions, based upon the physical distance between nodes, a mutual exchange of timecodes in such a regime would suffice for those nodes to authenticate one-another with absolute confidence.

Conclusion

By combining this novel approach with other, more traditional authentication modes, security may be enhanced and compromised protocols may be more easily identified.